## I. ISSUES RELATING TO THE CITED ART

Claims 1, 3, 6, 7, 9-11, 26-30, 32-35, and 37-38 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 5,790,548 issued to Sistanizadeh et al. ("*Sistanizadeh*"). This rejection is respectfully traversed.

Claims 4 and 5 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Sistanizadeh* in view of U.S. Patent Publication No. 2002/0026573 to Park ("*Park*"). This rejection is respectfully traversed.

Claims 8, 31, and 36 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over *Sistanizadeh* in view of U.S. Patent No. 6,782,422 issued to Bahl et al. ("*Bahl*"). This rejection is respectfully traversed.

### A. CLAIM 1

Claim 1 recites:

> A method of assigning a network address to a host based on authentication for a physical connection between the host and an intermediate device, the method comprising the computer-implemented steps of:
> receiving, at a router hosting an authenticator process for the host, from a first server that provides authentication and authorization, in response to a request for authentication for the physical connection, first data indicating at least some of authentication and authorization information;
> **receiving, at a DHCP relay agent process of the router,** from the host, a DHCP discovery message for discovering a logical network address for the host;
> **generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data; and**
> **sending the second message from the DHCP relay agent process to a DHCP server that provides the logical network address for the host;**
> **wherein generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data**. (emphasis added)

At least the above-bolded features of Claim 1 are not taught or suggested by *Sistanizadeh*.

*1.* Sistanizadeh *fails to teach or suggest the recited DHCP relay agent*

The final Office action cites col. 9, line 61 to col. 10, line 14 of *Sistanizadeh* for disclosing the step of "receiving, at a DHCP relay agent process of the router, from the host, a DHCP discovery message for discovering a logical network address for the host," as recited in Claim 1. This is incorrect. That portion of *Sistanizadeh* merely states that a DHCP server receives an IP address request from a computer, authenticates the computer, and sends the computer an IP address. The only mention of a router comes after the DHCP server sends the IP address to the computer. The applicable portion of *Sistanizadeh* states: "The router receives a packet from a computer, routes the packet to the appropriate ISP based on its source IP address, i.e., the computer's IP address" (col. 10, lines 4-6). However, according to Claim 1, a router receives a DHCP discovery message.

In the Response to Arguments section, the Final Office Action asserts that the Ethernet switch of *Sistanizadeh* (col. 13, lines 50-54) could be the recited DHCP relay agent merely because applicants' specification defines a DHCP relay agent as a process that executes on an intermediate device to forward DHCP messages between DHCP client and DHCP server (page2). However, Claim 1 recites features of the DHCP relay agent that are not taught or suggested by *Sistanizadeh*. For example, the DHCP relay agent is of the **same router** that hosts an authenticator process, whereas the Ethernet switch of *Sistanizadeh* does not host such an authenticator process. As another example, the DHCP relay agent receives, from an authenticator process of the same router, a message that contains authentication and authorization (AA) information, whereas the Ethernet switch of *Sistanizadeh* does not receive such a message, much less a message from a process hosted by the same router. As yet another example, the DHCP relay agent **generates a message** (i.e., the recited second message) that comprises a DHCP discovery message and the recited first data, whereas the Ethernet switch of

*Sistanizadeh* does not **generate** any message, much less a message that comprises a DHCP discovery message and AA information.

2. Sistanizadeh *fails to teach or suggest the recited second message*

The Final Office Action cites col. 12, line 31 to col. 13, line 56 of *Sistanizadeh* for disclosing the step of "generating at the DHCP relay agent process a second message that comprises the DHCP discovery message and the first data," as recited in Claim 1. This is incorrect. That cited portion of *Sistanizadeh* fails to even mention routers, much less anything resembling a DHCP relay agent process of a router. Therefore, *Sistanizadeh* must fail to teach or suggest that a process on a router generates a message, much less a message that comprises a DHCP discovery message and AA information, as recited in Claim 1. Fundamentally, *Sistanizadeh* only discloses a router that routes packets and deletes information from packets. None of the routers in *Sistanizadeh* **generate** messages that comprise information from two different sources (i.e., the recited first server and the recited host).

In the Response to Arguments section, the Final Office Action quotes col. 16, lines 40-47 of *Sistanizadeh* for disclosing the recited second message of Claim 1. However, that cited portion merely states:

> A Wide Area Network-Maintenance Administration Center (WAN-MAC) will monitor the Gateway Router, Ethernet Switch and have visibility of the ADSL equipment. As previously described with reference to the Access Architecture, ADSL Alarm information is collected via the M&P Device and transmitted to a concentrator in the SNMP format. The SNMP messages are translated into TL1 and transmitted via the Packet Data network to the TNM-OSS.

The Final Office Action then asserts, "The SNMP messages would have been the second message of claim 1" (page 3). However, no where does *Sistanizadeh* teach or suggest that an SNMP message comprises (1) a DHCP discovery message and (2) AA information, as Claim 1 requires of the recited second message. Instead, SNMP messages are used to control and

monitor routers remotely from a network operations center (col. 8, lines 56-57). Further, "SNMP comprises simple and limited messages pertaining to communications between the client software running on a manager's computer and management agents. These messages allow read operations for monitoring systems, write operations for system control, and enable searching tables, as well as setting systems to report abnormal conditions" (col. 15, lines 10-16). Fundamentally, *Sistanizadeh* fails to teach or suggest a message that comprises **a DHCP discovery message** and **AA information**.

*3.* Sistanizadeh *fails to teach or suggest the "hand off"*

In the Response to Arguments section, the Final Office Action ignores the substantive argument that *Sistanizadeh* fails to teach or suggest the "hand off." Instead, the Final Office Action states that "it is noted that the features upon which applicant relies (i.e., 'hand off') are not recited in the rejected claim(s)" (page 3). However, representatives of the Applicants are not alleging that Claim 1 recites the phrase "hand off." Rather, as clearly explained in the last response, the phrase "hand off" is merely a shorthand for a claim limitation that *Sistanizadeh* lacks, "wherein generating the second message further comprises sending a third message, from the authenticator process to the relay agent process, that contains at least some of the authentication and authorization information based on the first data," as recited in Claim 1.

Thus, according to Claim 1, one process, hosted by a router, sends a message to another process of the same router. That message contains AA information. One benefit of this approach is that the DHCP server is relieved from having to re-authenticate a user as a condition for assigning an address. **There is no similar communication disclosed in *Sistanizadeh*.**

Furthermore, similar to the recited second message, the Final Office Action failed to equate any element in the nearly one and a half columns cited in *Sistanizadeh* (i.e., col. 12, line

31 to col. 13, line 56) with to the recited third message of Claim 1, i.e., a message, sent from one process hosted by a router to another process of the same router, that contains AA information.

Based on the foregoing, *Sistanizadeh* fails to teach or suggest all the limitations of Claim 1. Therefore, Claim 1 is patentable over *Sistanizadeh*. Reconsideration and withdrawal of the rejection of Claim 1 under 35 U.S.C. § 102(b) is therefore respectfully requested.

B. CLAIMS 26-28

Each of the features discussed above for Claim 1 is present in independent Claims 26-28. Therefore, Claims 26-28 are patentable for at least those reasons that Claim 1 is patentable as set forth above.

C. CLAIMS 3-8, 10-11, AND 29-38

Each of the features discussed above for Claim 1 is present, by dependency, in Claims 3-8, 10-11, and 29-38. Because each of the dependant claims includes the limitations of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable.

*1. Claim 10*

Additionally, Claim 10 depends on Claim 1 and further recites that "the first data includes user class data indicating a particular group of one or more authorized users of the host" (emphasis added). In rejecting Claim 10, the Final Office Action cites col. 12, line 31 to col. 13, line 56 of *Sistanizadeh*. However, the Final Office Action cites col. 17, lines 26-39 for disclosing the recited first data.

## II. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a law firm check for the petition for extension of time fee is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: January 30, 2008

/DanielDLedesma#57181/
Daniel D. Ledesma
Reg. No. 57,181

2055 Gateway Place Suite 550
San Jose, California 95110-1083
Telephone No.: (408) 414-1229
Facsimile No.: (408) 414-1076